

at least one element defining a protected processing environment,
a method of operating the appliance characterized by the step of storing and using permissions, methods, keys, programs and/or other information to electronically manage rights.

113. (NEW) A rights management appliance including at least one processor element at least in part defining a protected processing environment, characterized in that the protected processing environment stores and uses permissions, methods, keys, programs and/or other information to electronically manage rights.

114. (NEW) In a rights management appliance including at least one processor element at least in part defining a protected processing environment, a method comprising storing and using permissions, methods, keys, programs and/or other information to electronically manage rights.

115. (NEW) An electronic appliance arrangement containing a protected processing environment and at least one secure database operatively connected to said protected processing environment, said arrangement including means to monitor usage of at least one aspect of an amount of appliance usage and control said usage based at least in part upon protected appliance usage control information processed at least in part through use of said protected processing environment.

116. (NEW) In an electronic appliance arrangement containing a protected processing environment and at least one secure database operatively connected to said protected processing environment, a method characterized by the steps of monitoring usage of at least one aspect of appliance usage and controlling said usage based at least in part upon protected appliance usage control information processed at least in part through use of said protected processing environment.

117. (NEW) A secure component-based operating process including:
(a) retrieving at least one component;
(b) retrieving a record that specifies a component assembly;
(c) checking said component and/or said record for validity;

(d) using said component to form said component assembly in accordance with said record; and

(e) performing a process based at least in part on said component assembly.

118. (NEW) A secure component operating system process including:

receiving a component;

receiving directions specifying use of said component to form a component assembly;

authenticating said received component and/or said directions;

forming, using said component, said component assembly based at least in part on said received directions; and

using said component assembly to perform at least one operation.

119. (NEW) A method comprising performing the following steps within a secure operating system environment:

providing code;

providing directions specifying assembly of said code into an executable program;

checking said received code and/or said assembly directions for validity; and

in response to occurrence of an event, assembling said code in accordance with said received assembly directions to form an assembly for execution.

120. (NEW) A method for managing at least one resource with a secure operating environment, said method comprising:

securely receiving a first control from a first entity external to said operating environment;

securely receiving a second control from a second entity external to said operating environment, said second entity being different from said first entity;

securely processing, using at least one resource, a data item associated with said first and second controls; and

securely applying said first and second controls to manage said resource for use with said data item.

121. (NEW) A method for securely managing at least one operation on a data item performed at least in part by an electronic arrangement, said method comprising:

- (a) securely delivering a first procedure to said electronic arrangement;
- (b) securely delivering, to said electronic arrangement, a second procedure separable or separate from said first procedure;
- (c) performing at least one operation on said data item, including using said first and second procedures in combination to at least in part securely manage said operation; and
- (d) securely conditioning at least one aspect of use of said data item based on said delivering steps (a) and (b) having occurred.

71 122. (NEW) A method for securely managing at least one operation performed at least in part by a secure electronic appliance, comprising:

- (a) selecting an item that is protected with respect to at least one operation;
- (b) securely independently delivering plural separate procedures to said electronic appliance;
- (c) using said plural separate procedures in combination to at least in part securely manage said operation with respect to said selected item; and
- (d) conditioning successful completion of said operation on said delivering step (b) having occurred.

123. (NEW) A method for processing based on independent deliverables comprising:

- securely delivering a first piece of code defining a first part of a process;
- separately, securely delivering a second piece of code defining a second part of said process;
- ensuring the integrity of the first and second delivered pieces of code; and
- performing said process based at least in part on said first and second delivered code pieces.

124. (NEW) A method of securely controlling at least one protected operation with respect to a data item comprising:

- (a) supplying at least a first control from a first party;
- (b) supplying at least a second control from a second party different from said first party;
- (c) securely combining said first and second controls to form a set of controls;
- (d) securely associating said control set with said data item; and
- (e) securely controlling at least one protected operation with respect to said data item based on said control set.

125. (NEW) A secure method for combining data items into a composite data item comprising:

- (a) securely providing a first data item having at least a first control associated therewith;
- (b) securely providing a second data item having at least a second control associated therewith;
- (c) forming a composite of said first and second data items;
- (d) securely combining said first and second controls into a composite control set; and
- (e) performing at least one operation on said composite of said first and second data items based at least in part on said composite control set.

126. (NEW) A secure method for controlling a protected operation comprising:

- (a) delivering at least a first control and a second control; and
- (b) controlling at least one protected operation based at least in part on a combination of said first and second controls, including at least one of the following steps:

resolving at least one conflict between said first and second controls based on a predefined order;

providing an interaction with a user to form said combination; and
dynamically negotiating between said first and second controls.

127. (NEW) A secure method comprising:
selecting protected data;
extracting said protected data from an object;
identifying at least one control to manage at least one aspect of use of said
extracted data;
placing said extracted data into a further object; and
associating said at least one control with said further object.

128. (NEW) A secure method of modifying a protected object comprising:
(a) providing a protected object; and
(b) embedding at least one additional element into said protected object
without unprotecting said object.

129. (NEW) A method for managing at least one resource with a secure operating
environment, said method comprising:
securely receiving a first load module from a first entity external to said
operating environment;
securely receiving a second load module from a second entity external to said
operating environment, said second entity being different from said first entity;
securely processing, using at least one resource, a data item associated with
said first and second load modules; and
securely applying said first and second load modules to manage said resource
for use with said data item.

130. (NEW) A method for negotiating electronic contracts, comprising:
receiving a first control set from a remote site;
providing a second control set;
performing, within a protected processing environment, an electronic
negotiation between said first control set and said second control set, including
providing interaction between said first and second control sets; and
producing a negotiated control set resulting from said interaction between said
first and second control sets.

131. (NEW) A system for supporting electronic commerce including:
means for creating a first secure control set at a first location;
means for creating a second secure control set at a second location;
means for securely communicating said first secure control set from said first location to said second location; and
means at said second location for securely integrating said first and second control sets to produce at least a third control set comprising plural elements together comprising an electronic value chain extended agreement.

DI 132. (NEW) A system for supporting electronic commerce including:
means for creating a first secure control set at a first location;
means for creating a second secure control set at a second location;
means for securely communicating said first secure control set from said first location to said second location; and
negotiation means at said second location for negotiating an electronic contract through secure execution of at least a portion of said first and second secure control sets.

133. (NEW) A secure component-based operating system including:
component retrieving means for retrieving at least one component;
record retrieving means for retrieving a record that specifies a component assembly;
checking means, coupled to said component retrieving means and said record retrieving means, for checking said component and/or said record for validity;
using means, coupled to said checking means, for using said component to form said component assembly in accordance with said record; and
performing means, coupled to said using means, for performing a process based at least in part on said component assembly.

134. (NEW) A secure component-based operating system including:
a database manager that retrieves, from a secure database, at least one component and at least one record that specifies a component assembly;
an authenticating manager that checks said component and/or said record for validity;
a channel manager that uses said component to form said component assembly in accordance with said record; and
an execution manager that performs a process based at least in part on said component assembly.

DI 135. (NEW) A secure component operating system including:
means for receiving a component;
means for receiving directions specifying use of said component to form a component assembly;
means, coupled to said receiving means, for authenticating said received component and/or said directions;
means, coupled to said authenticating means, for forming, using said component, said component assembly based at least in part on said received directions; and
means, coupled to said forming means, for using said component assembly to perform at least one operation.

136. (NEW) A secure component operating environment including:
a storage device that stores a component and directions specifying use of said component to form a component assembly;
an authenticating manager that authenticates said component and/or said directions;
a channel manager that forms, using said component, said component assembly based at least in part on said directions; and
a channel that executes said component assembly to perform at least one operation.

137. (NEW) A secure operating system environment comprising:
a storage device that stores code and directors specifying assembly of said code into an executable program;
a validating device that checks said received code and/or said assembly directors for validity; and
an event-driven channel that, in response to occurrence of an event, assembles said code in accordance with said assembly directions to form an assembly for execution.

DI 138. (NEW) A secure operating environment system for managing at least one resource comprising:
a communications arrangement that securely receives a first control from a first entity external to said operating environment, and securely receives a second control from a second entity external to said operating environment, said second entity being different from said first entity; and
a protected processing environment, coupled to said communications arrangement, that:
(a) securely processes, using at least one resource, a data item associated with said first and second controls, and
(b) securely applies said first and second controls to manage said resource for use of said data item.

139. (NEW) A system for negotiating electronic contracts, comprising:
a storage arrangement that stores a first control set received from a remote site, and stores a second control set;
a protected processing environment, coupled to said storage arrangement, that:
(a) performs an electronic negotiation between said first control set and said second control set,
(b) provides interaction between said first and second control sets, and
(c) produces a negotiated control set resulting from said interaction between said first and second control sets.

140. (NEW) A method for supporting electronic commerce including:
creating a first secure control set at a first location;
creating a second secure control set at a second location;
securely communicating said first secure control set from said first location to
said second location; and

electronically negotiating, at said second location, an electronic contract,
including the step of securely executing at least a portion of said first and second
secure control sets.

141. (NEW) An electronic appliance comprising:

a processor; and

at least one memory device connected to said processor;

wherein said processor includes:

retrieving means for retrieving at least one component, and at least one
record that specifies a component assembly, from said memory device,

checking means coupled to said retrieving means for checking said
component and/or said record for validity, and

using means coupled to said retrieving means for using said component
to form said component assembly in accordance with said record.

142. (NEW) An electronic appliance comprising:

at least one processor;

at least one memory device connected to said processor; and

at least one input/output connection coupled to said processor,

wherein said processor at least in part executes a rights operating
system to provide a secure operating environment within said electronic
appliance.

143. (NEW) A method for auditing the use of at least one resource with a secure operating environment, said method comprising:

securely receiving a first control from a first entity external to said operating environment;

securely receiving a second control from a second entity external to said operating environment, said second entity being different from said first entity;

using at least one resource;

securely sending to said first entity in accordance with said first control, first audit information concerning use of said resource; and

securely sending to said second entity in accordance with said second control, second audit information concerning use of said resource, said second audit information being at least in part different from said first audit information.

144. (NEW) A method for auditing the use of at least one resource with a secure operating environment, said method comprising:

securely receiving first and second control alternatives from an entity external to said operating environment;

selecting one of said first and second control alternatives;

using at least one resource;

if said first control alternative is selected by said selecting step, securely sending to said entity in accordance with said first control alternative, first audit information concerning use of said resource; and

if said second control alternative is selected by said selecting step, securely sending to said second entity in accordance with said second control alternative, second audit information concerning use of said resource, said second audit information being at least in part different from said first audit information.